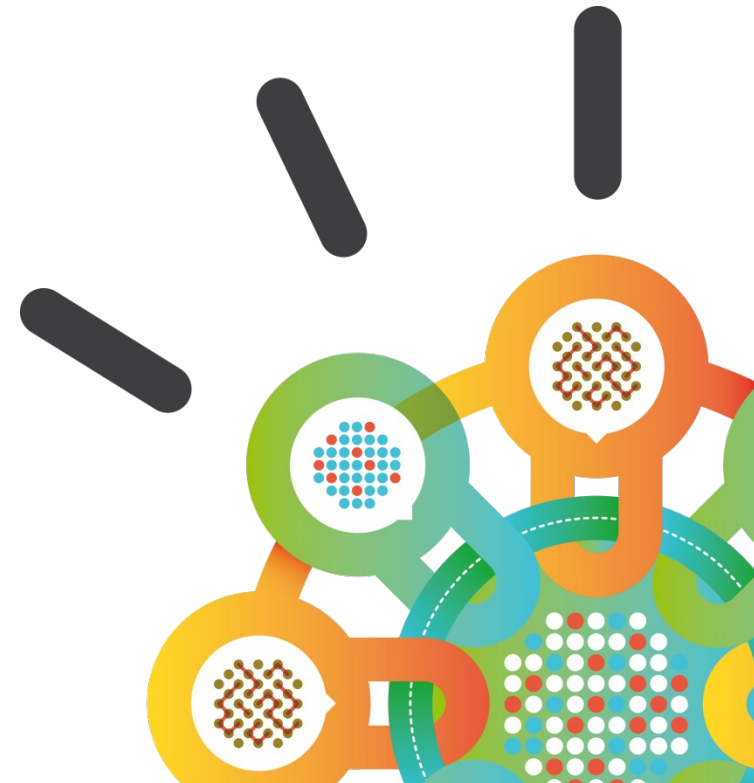


Security Intelligence.
Think Integrated.

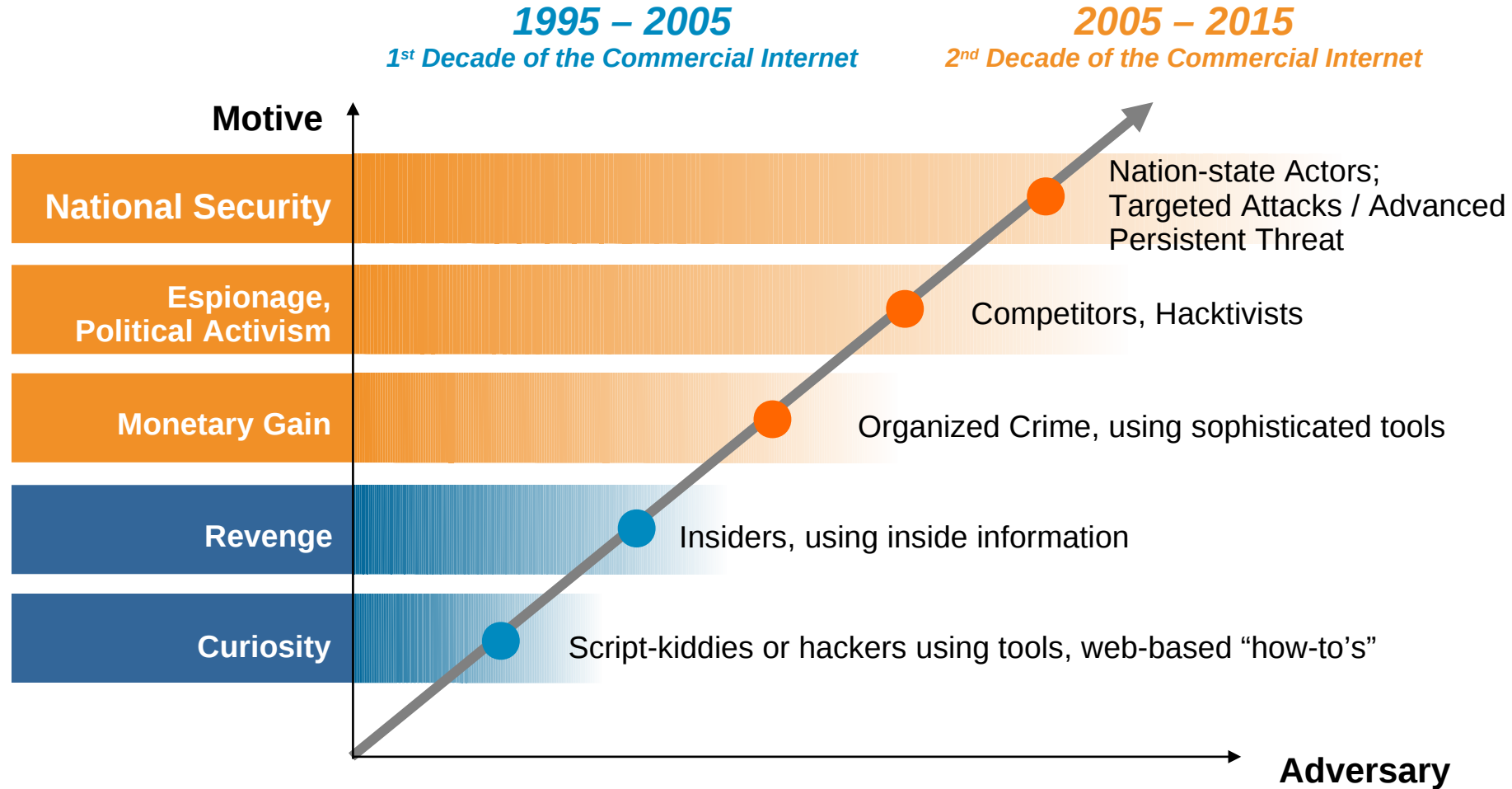
Security from the (Product Development) Trenches

October 2012

Dr Paul Ashley
IBM Security Systems Division



Advanced Threats: The sophistication of Cyber threats, attackers and motives is rapidly escalating





Anonymous hackers cripple Australian websites

ANDREW COLLEY [The Australian](#) July 24, 2012 2:49PM 2 comments



"Your government seems to think that everyone in Australia is a terrorist." The government sites targeted appear to be concentrated in Queensland ... They include the state's tourism web site, ...

Israeli Hackers Hit Saudi Stock Exchange

Israeli hackers **quickly retaliated yesterday** against Monday's online disruption of the Tel Aviv Stock Exchange and El Al Airlines' websites by launching a counterstrike, taking down the websites of the Saudi Stock Exchange and the Abu Dhabi Securities Exchange.

The federal government's e-health platform hacked at birth

FRAN FOO [The Australian](#) July 03, 2012 12:00AM

THE federal government's e-health platform was hacked while being developed but the incident went undetected for several months.

The revelation comes after Accenture, the main contractor for the personally controlled e-health record program, delayed delivery, resulting in only 40 per cent of the system being ready by its July 1 launch date.

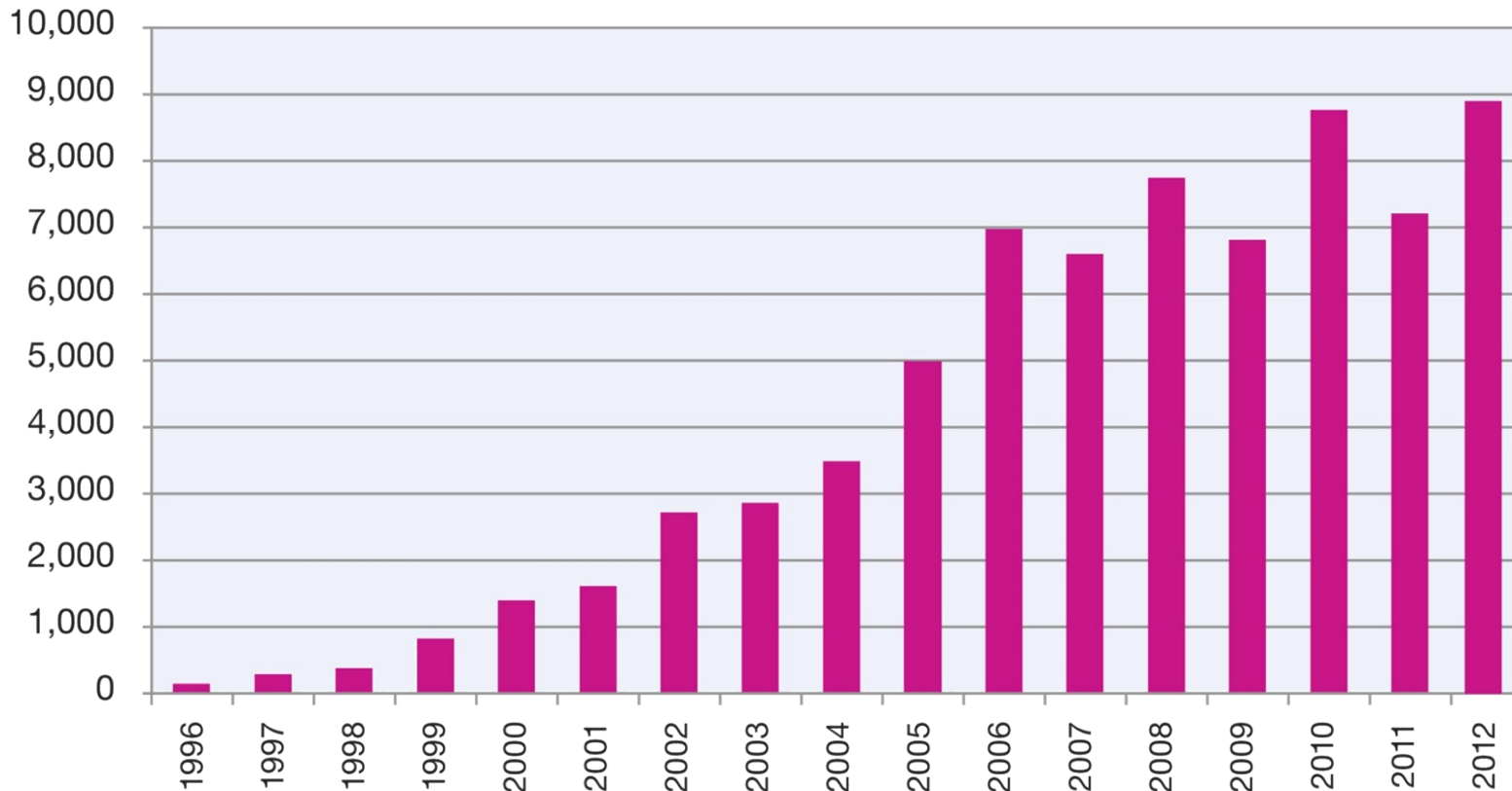
The hacking incident raises issues of reliability and security of the system as people start to register for an e-health record that would contain their personal details and health information such as medications, allergies and immunisation details.

Vulnerability disclosures up in 2012



- Total number of vulnerabilities grew (4,400 in 1H 2012) – the projection could reach all time high in 2012

Vulnerability Disclosures Growth by Year
1996-2012 (projected)

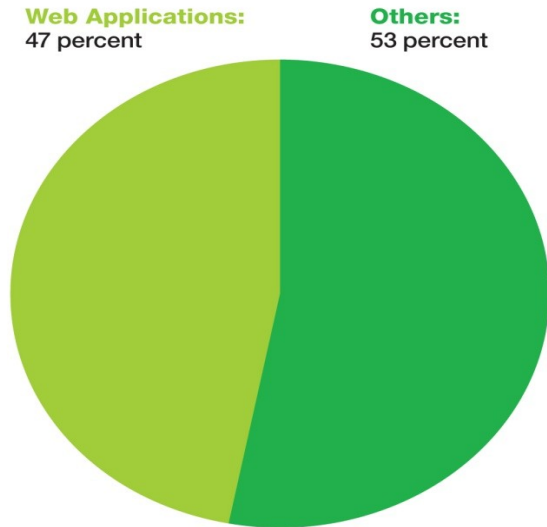


Web Application Vulnerabilities Rise Again



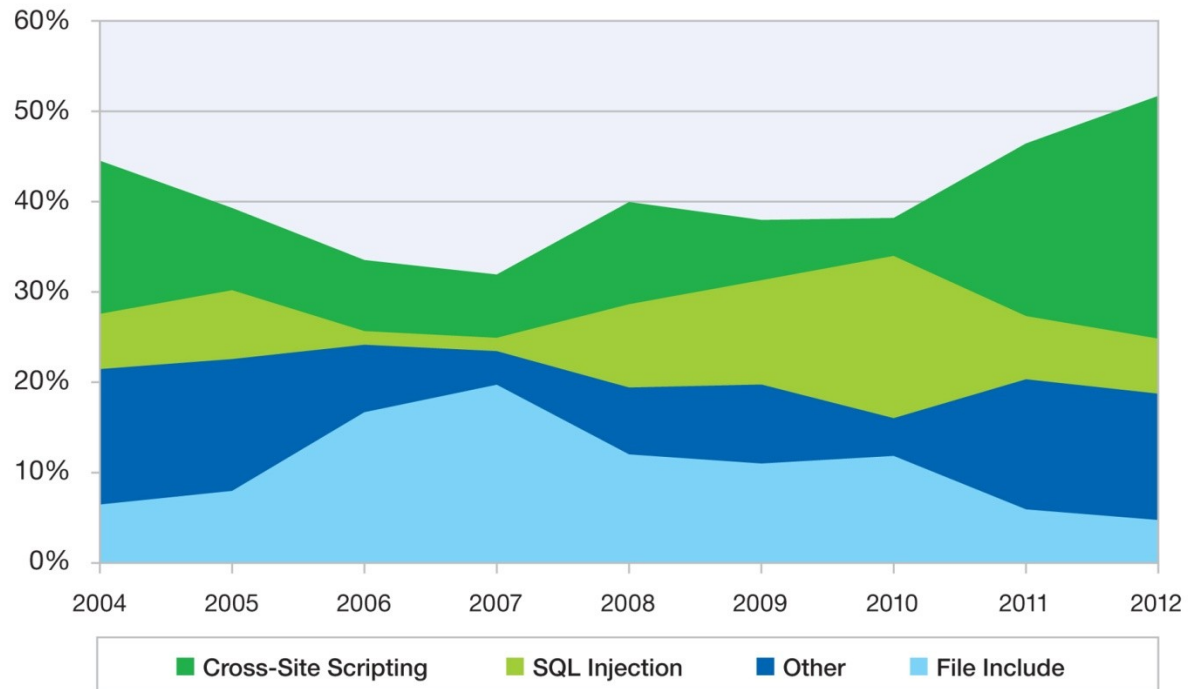
- At mid-year 2012, 47% of security vulnerabilities affected web applications
 - Up from 41% in 2011
 - XSS reaches high of 51%

Web Application Vulnerabilities
as a Percentage of All Disclosures in 2012 H1



Web Application Vulnerabilities by Attack Technique

2004-2012 H1

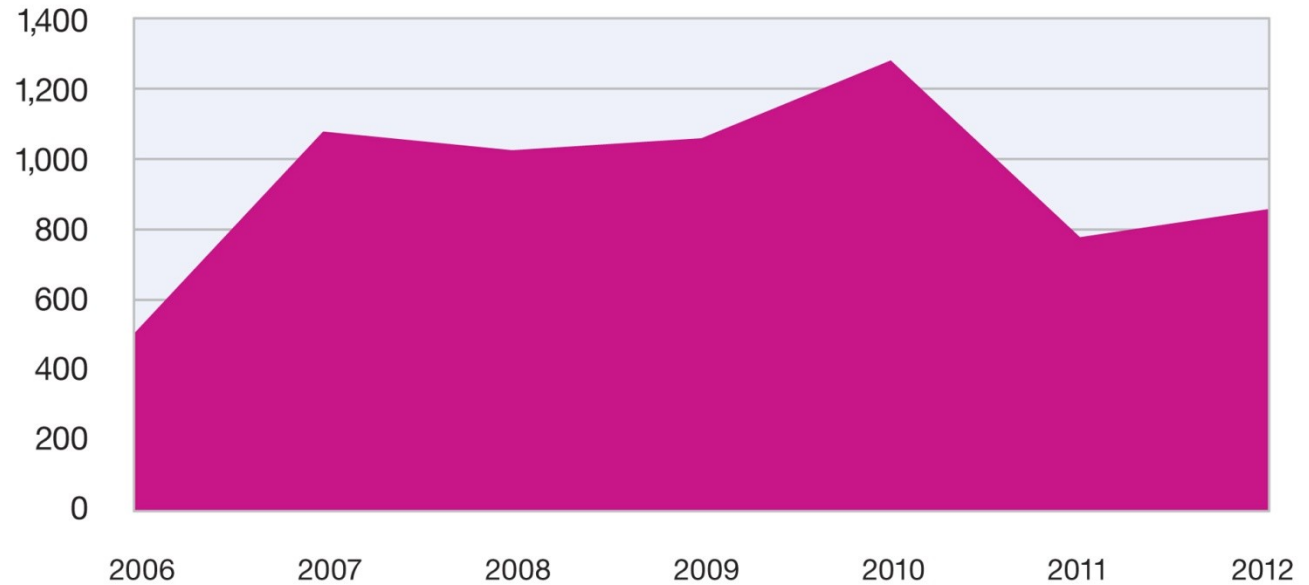


Public Exploit Disclosures



True Exploit Disclosures
2006-2012 H1 (projected)

- Decrease in percentage of vulnerabilities
- Slightly up in actual numbers compared to 2011



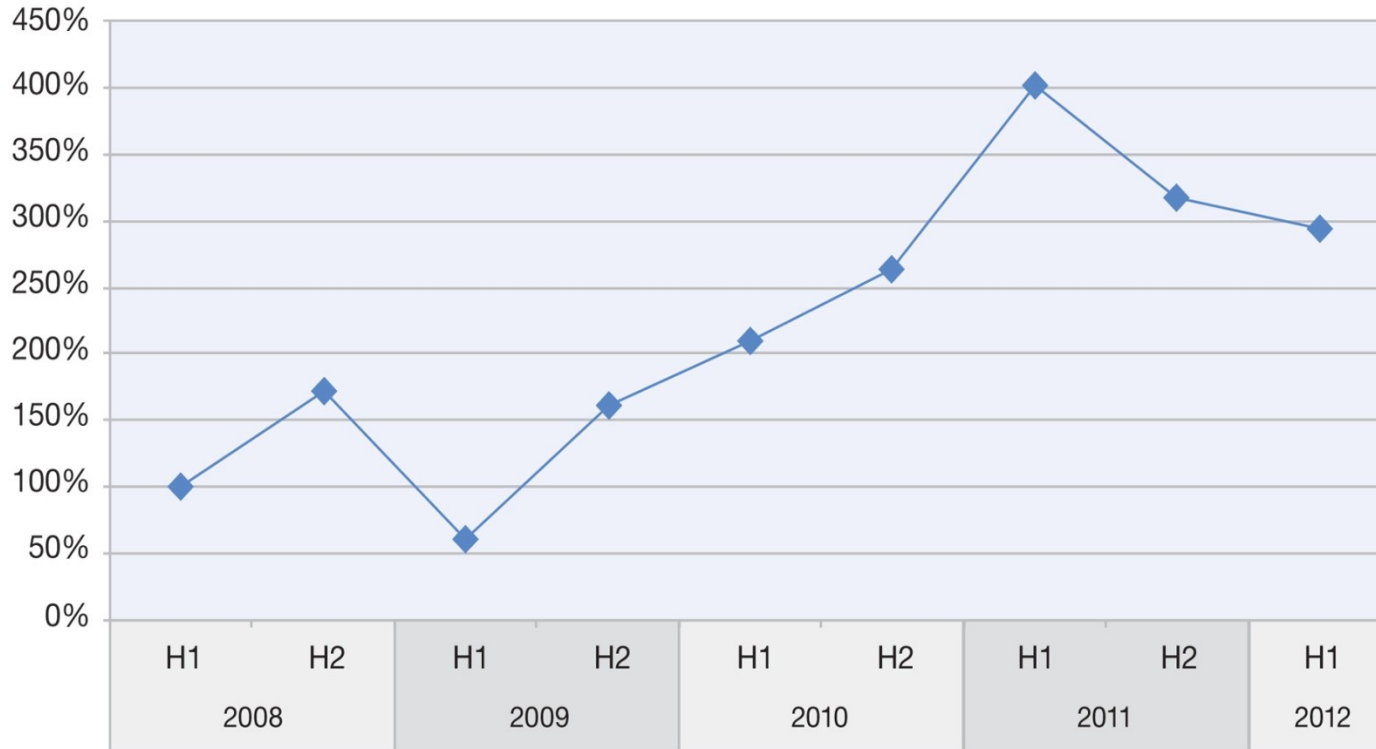
	2006	2007	2008	2009	2010	2011	2012
True Exploits	504	1078	1025	1059	1280	778	858
Percent of Total	7.3%	16.5%	13.3%	15.7%	14.7%	10.9%	9.7%

Source: IBM X-Force® Research and Development

Anonymous Proxies Still used to Bypass Web Filtering



Volume of Newly Registered Anonymous Proxy Websites
2008 H1 to 2012 H1



Source: IBM X-Force® Research and Development

MAC Platforms Continue to Draw Attention

Flashback

- First variant discovered in September of 2011.
- 2012 variants were somewhat special
 - Employed drive-by-download techniques through compromised Wordpress blog sites
 - Works around this by using multi-platform exploits through Java vulnerabilities.
 - The Apple version of Java was updated later than Oracle: 600,000 infections estimated.



Mac APT

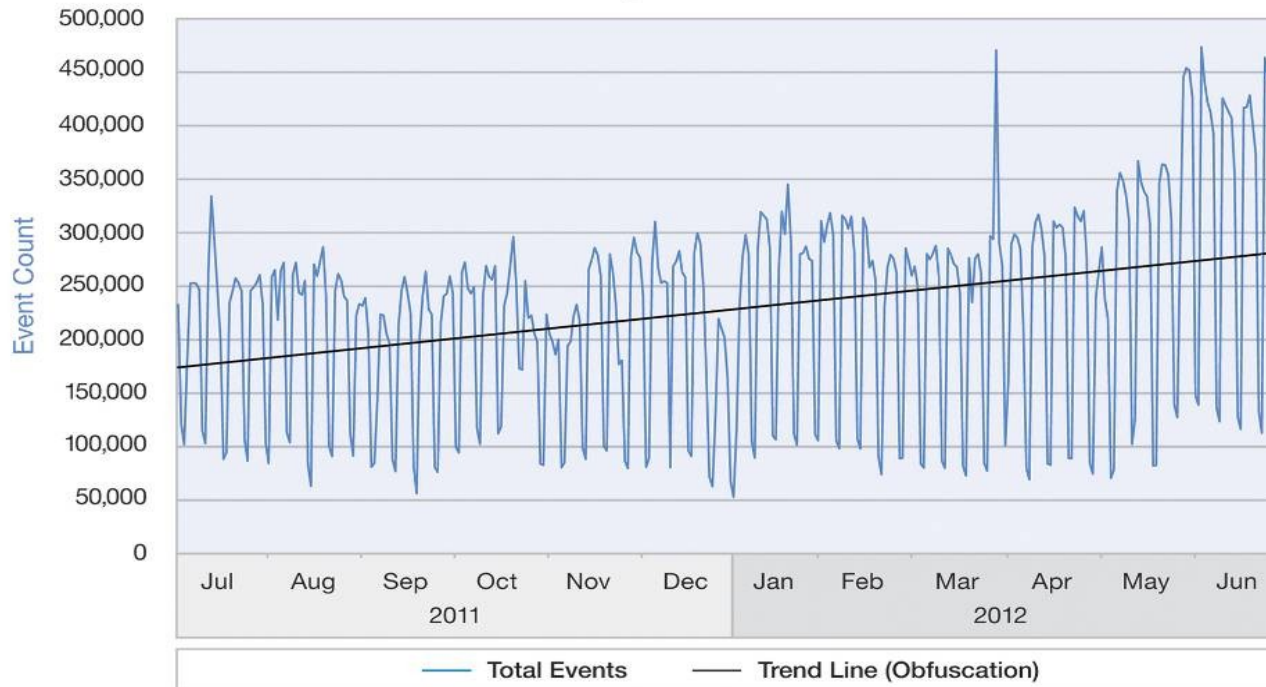
- Tibet malware discovered in March.
 - The first variants used Java exploit to spread.
 - Next variants use an MS Word vulnerability that affects the 2004 and 2008 versions of Word for Mac
- SabPub backdoor discovered in April.
 - The first variant did not initially show any sign that it was a targeted attack
 - Uses the same Java exploit as Flashback
 - The next variant is similar to the Tibet malware (using Word)

Obfuscation Events Growing



Obfuscation is a technique to hide or mask the sources and methods of a security relevant event. New obfuscation methods are constantly evolving in an attempt to evade intrusion prevention systems (IPS) and anti-virus software.

MSS Growth of Obfuscation Technique
July 2011 to June 2012



The challenging state of network security



Stealth Bots • Targeted Attacks
Worms • Trojans • Designer Malware

SOPHISTICATED ATTACKS

Increasingly sophisticated attacks are using multiple attack vectors and increasing risk exposure



STREAMING MEDIA

Streaming media sites are consuming large amounts of bandwidth



SOCIAL NETWORKING

Social media sites present productivity, privacy and security risks including new threat vectors

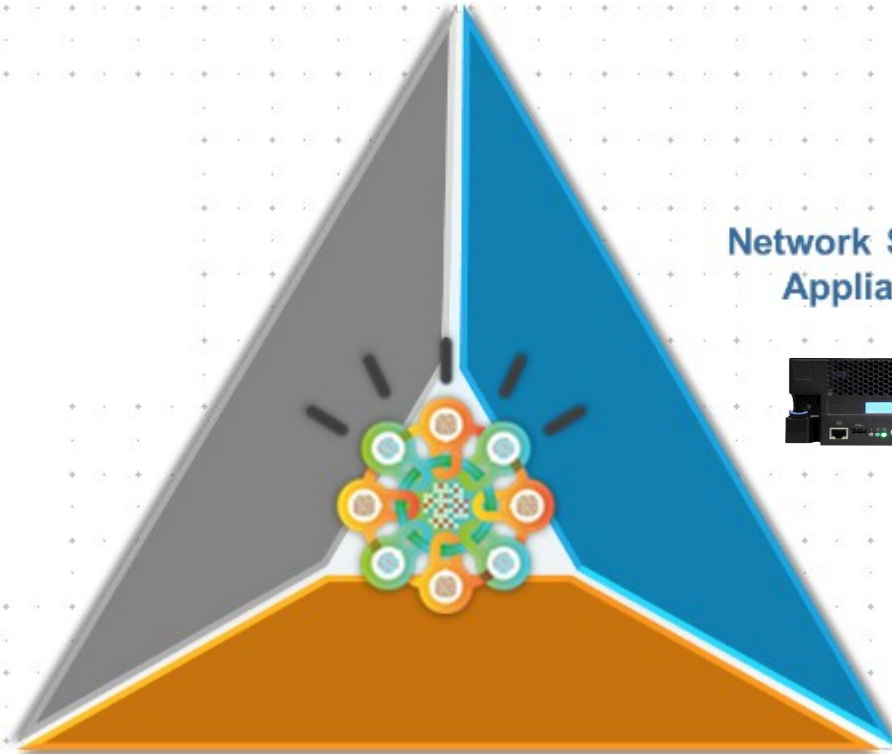


URL Filtering • IDS / IPS
IM / P2P • Web App Protection
Vulnerability Management

POINT SOLUTIONS

Point solutions are siloed with minimal integration or data sharing

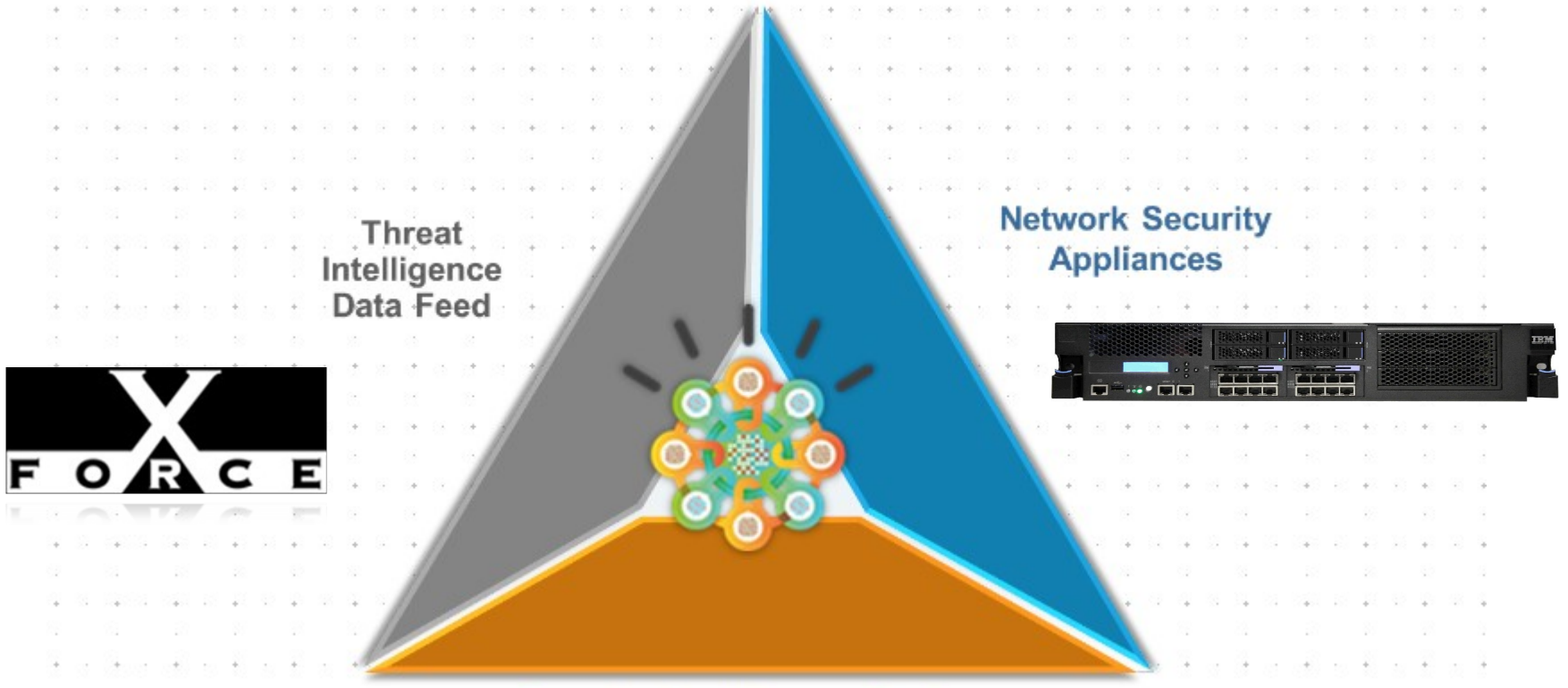
Vision for Advanced Threat Protection



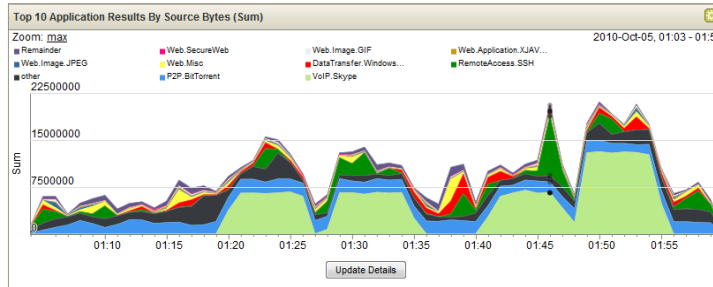
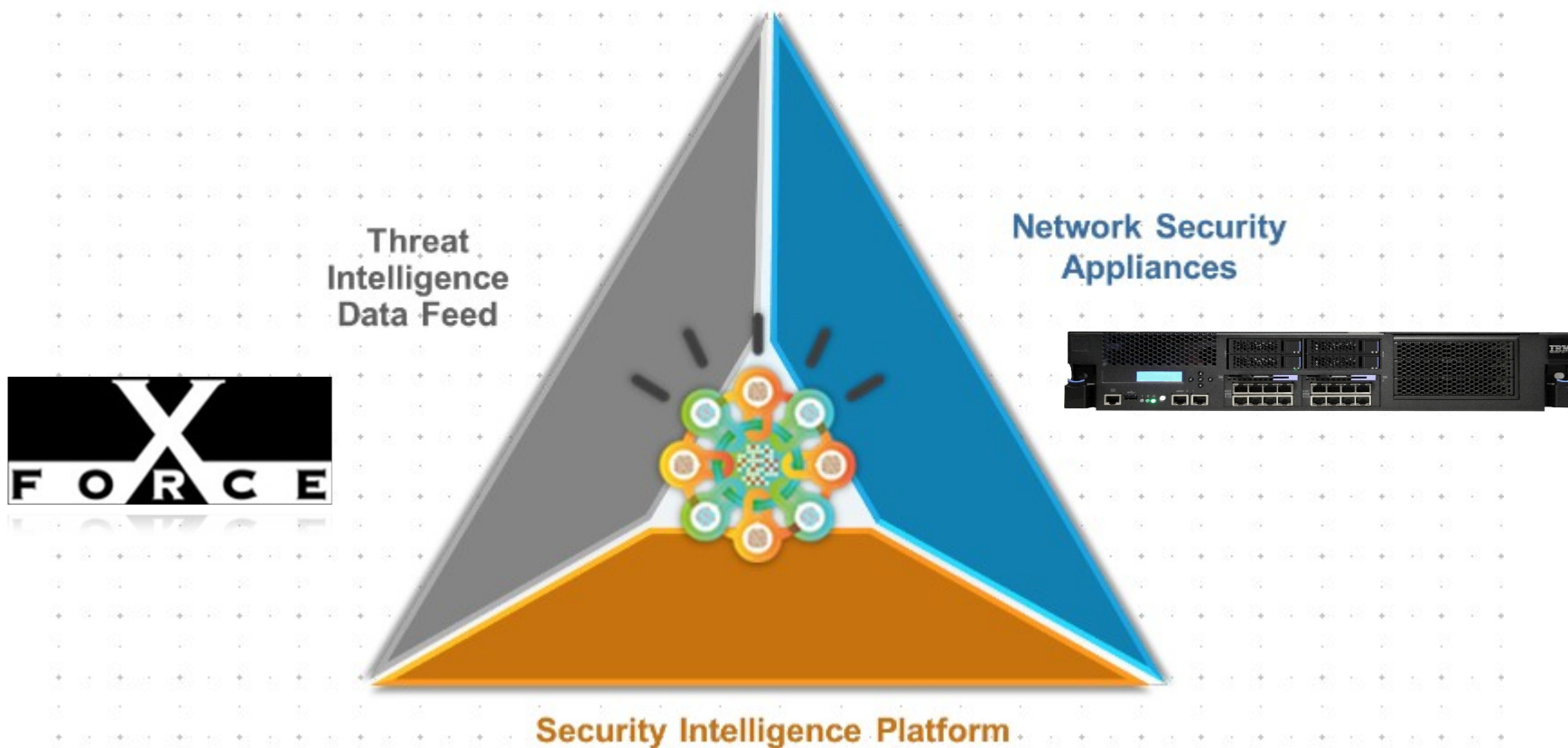
Network Security
Appliances



Vision for Advanced Threat Protection



Vision for Advanced Threat Protection



X-Force Threat Intelligence Sources



X-Force Threat Intelligence Sources

IBM Managed Security Services

20,000+ devices under management

3,700+ managed clients worldwide

13B+ events managed per day

133 monitored countries



IBM Research

Security Information

17B analyzed web pages & images

40M spam & phishing attacks

68K documented vulnerabilities

Millions of unique malware samples

How to protect today's networks from tomorrow's threats

- Server
- Network
- Geography
- Reputation
- User or Group



- Web Category Protection
- Access Control
- Protocol Aware Intrusion Protection
- Client-Side Protection
- Botnet Protection
- Network Awareness
- Web Protection
- Reputation

- Allow marketing and sales teams to access social networking sites
- Block attachments on all outgoing emails and chats
- A more strict security policy is applied to traffic from countries where I do not do business
- Advanced inspection of web application traffic destined to my web servers
- Block known botnet servers and phishing sites
- Allow, but don't inspect, traffic to financial and medical sites

Who

What

Controls

Security

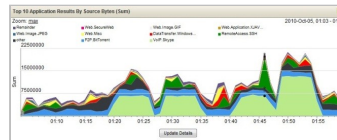
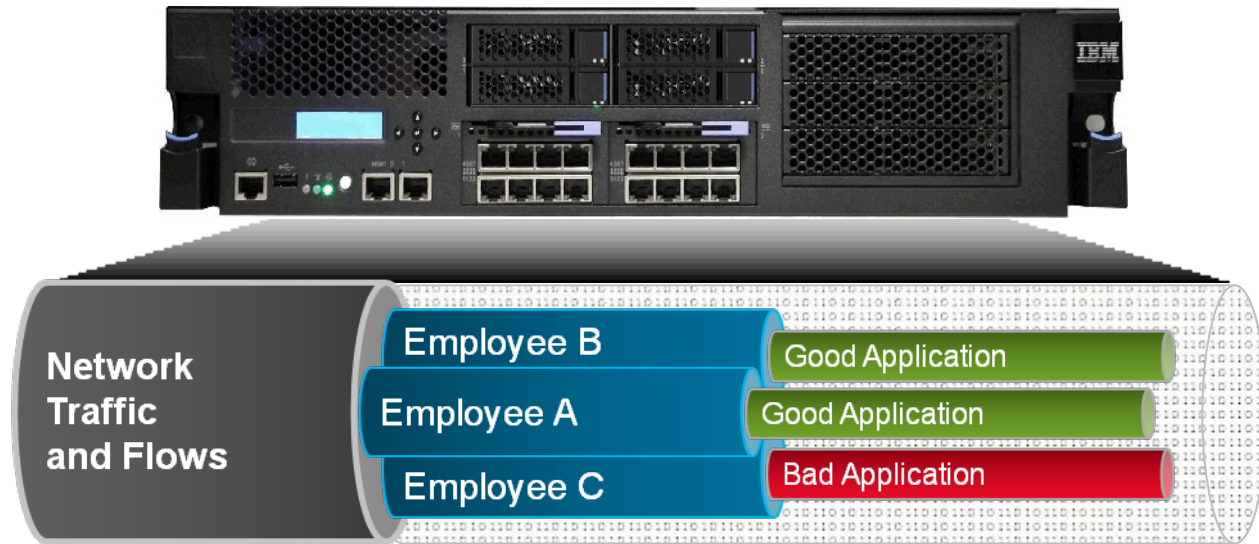
172.29.230.15, 192.168.0.0/16

80, 443, 25, 21, 2048-65535



Visibility: Understanding Who, What and When

- **Immediately discover** which applications and web sites are being accessed
- **Quickly Identify misuse** by application, website, user, and group
- **Understand who and what** are consuming bandwidth on the network
- **Superior detection of advanced threats** through integration with security intelligence for network anomaly and event details



Network flows can be sent to security intelligence for enhanced analysis, correlation and anomaly detection

Identity context ties users and groups with their network activity - going beyond IP address only policies

Application context fully classifies network traffic, regardless of port, protocol or evasion techniques

Increase Security ● Reduce Costs ● Enable Innovation

"We were able to detect the Trojan "Poison Ivy" within the first three hours of deploying IBM Security Network Protection"

– Australian Hospital

Complete Control: Overcoming a Simple Block-Only Approach

- Control network access by users, groups, systems, protocols, applications & application actions
- Block evolving, high-risk sites** such as Phishing and Malware with constantly updated categories
- Comprehensive up-to-date web site coverage** with industry-leading 17 Billion+ URLs (*50-100x the coverage comparatively*)
- Rich application support** with 1000+ applications and individual actions



IBM Security Network Protection

Home Appliance Dashboard Monitor Analysis and Diagnostics Secure Policy Configuration Manage System Settings Deploy 3

Network Access Policy

Order	Enable	Source	Destination	Application	Action	Alert	Inspection	Schedule	Comment
1	<input checked="" type="checkbox"/>	Any	Any	DHCP1	Accept		Default IPS		Allow DHCP
2	<input checked="" type="checkbox"/>	Unauthorized	Any	Any	Authenticate (Reject)		Default IPS		CaptivePortal
3	<input checked="" type="checkbox"/>	Any	LMI	Any	Accept		Default IPS		All LMI access
4	<input checked="" type="checkbox"/>	Any	Search	Any	Accept		Default IPS		Full Web Access
5	<input checked="" type="checkbox"/>	HR	Any	SocialNetworking	Accept		Default IPS		Allow HR
6	<input checked="" type="checkbox"/>	Internal	Any	GoodURLs	Accept		Default IPS		White list
7	<input checked="" type="checkbox"/>	Internal	Any	BadSites BitTorrents Movies	Reject	Local Log	Default IPS		Block bad sites

Limit the use of social networking, file sharing, and web mail for common users

Allow full access to social networking sites for marketing and HR teams`

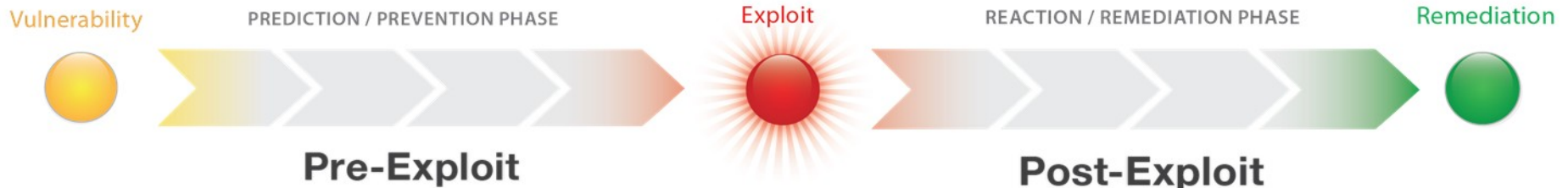
Stop broad misuse of the corporate network by blocking sites that introduce undue risk and cost

Flexible network access control policies

"We had a case in Europe where workers went on strike for 3 days after Facebook was completely blocked...so granularity is key."

– SecureDevice

Security Intelligence: Pre and Post Exploit



Prediction & Prevention

Risk Management. Vulnerability Management.
 Configuration and Patch Management.
 X-Force Research and Threat Intelligence.
 Compliance Management. Reporting and Scorecards.

Reaction & Remediation

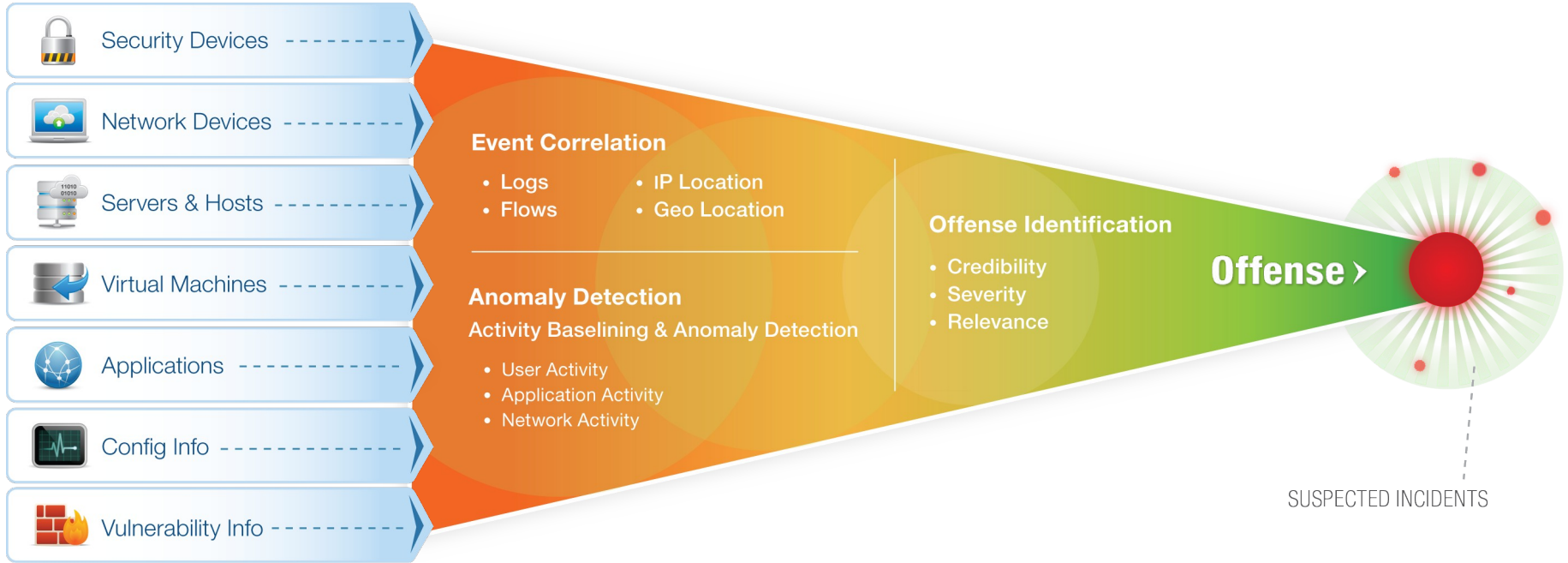
Network and Host Intrusion Prevention.
 Network Anomaly Detection. Packet Forensics.
 Database Activity Monitoring. Data Leak Prevention.
 SIEM. Log Management. Incident Response.



Security Intelligence



Data Reduction & Prioritization



Most Sources
+
Most Intelligence
=
Most Accurate & Actionable Insight

Data Reduction & Prioritization

System Summary

Current Flows Per Second	1.4M
Flows (Past 24 Hours)	1.3M
Current Events Per Second	17,384
New Events (Past 24 Hours)	677M
Updated Offenses (Past 24 Hours)	588
Data Reduction Ratio	10633 : 1

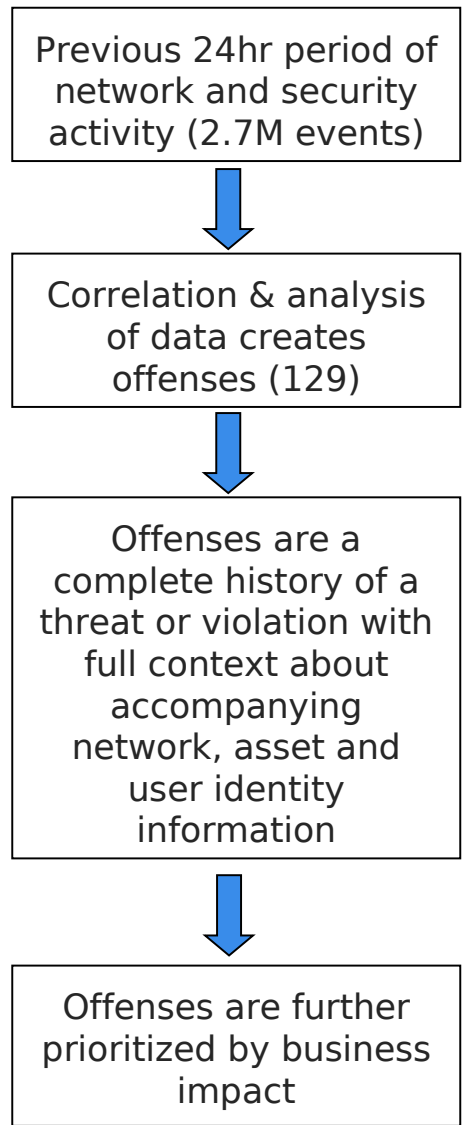
Most Recent Offenses

Offense Name	Magnitude
Local Web Scanner Detected containing Web.Image.GIF	[Progress bar]
Potential P2P Traffic or VoIP Detected preceded by Local TCP Scanner Detected containing unknown	[Progress bar]
Local Web Scanner Detected containing Web.Image.JPEG	[Progress bar]
MS SMB2 Validate Provider Callback RCE	[Progress bar]
Local Web Scanner Detected containing Web.HTTPWeb	[Progress bar]

Default-IDS / IPS-All: Top Alarm Signatures (Event C)

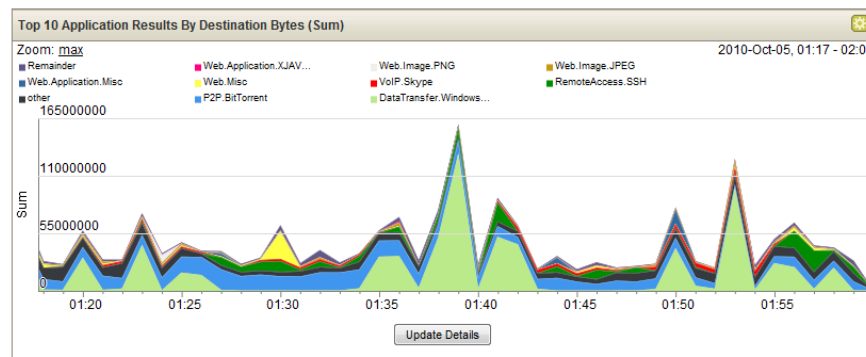
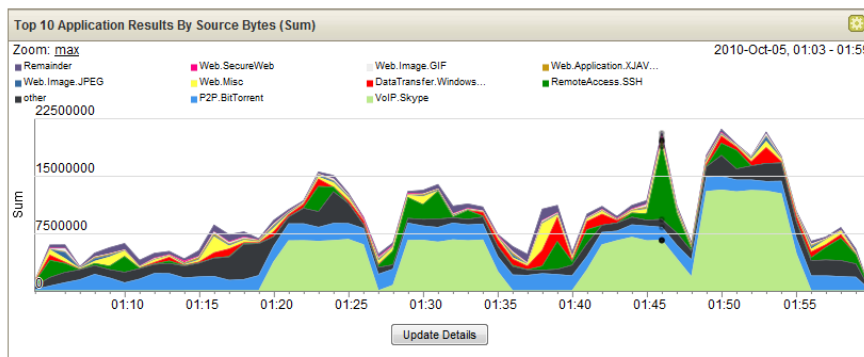
Zoom: max 2010-Oct

Legend: Remainder (yellow), HTTP: HTTP on non-st (red), MISC: CONEXANT-LOGIN (green), Slapper Worm (black), HTTP: HOTMAIL: EXE-DOW... (blue), Juniper Networks Int... (light green)



Flows for Network Intelligence

- Policy monitoring and rogue server detection
- Visibility into all attacker communication
- Passive flow monitoring builds asset profiles & auto-classifies hosts



(Hide Charts)

Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum)	Source Packets (Sum)	Destination Packets (Sum)	Total Packets (Sum)	Count
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708	547 851 023	178 629	390 655	569 284	123
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654	235 838 522	127 854	161 966	289 820	546
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101	206 151 800	93 672	228 533	322 205	6 810
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290	177 991 748	195 570	76 007	271 577	171
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020	149 113 136	101 404	261 727	363 131	122
Web.Misc	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741	31 361 821	33 634	23 904	57 538	2 401
Web.Application.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267	23 780 010	8 193	15 674	23 867	89
Web.Image.JPEG	Multiple (13)	Multiple (4)	Multiple (60)	80	other	2 418 857	18 538 204	20 957 061	15 449	14 150	29 599	586
Web.Web.Misc	Multiple (46)	Multiple (4)	Multiple (160)	80	other	266 544	6 427 264	6 693 808	4 484	6 830	11 314	764

Displaying 1 to 40 of 64 items (Elapsed time: 0:00:00.106)

Network Anomaly Detection

- **Network Anomaly Detection** provides deep network visibility and real-time insight to identify and remediate threats
- Network behavioral analytics improves proficiency in proactive controls
- Integrated analysis of network flow data brings additional security intelligence:
 - Correlation of Threat & Data flow for **enhanced incident analysis**
 - Network Activity Monitoring to **profile user and system behavior to improve threat intelligence**
- Includes support for **identity sources** to associate user activity with incidents; and support for **vulnerability data** to correlate attack with vulnerable assets



Network Behavior
Awareness

Identity
Awareness

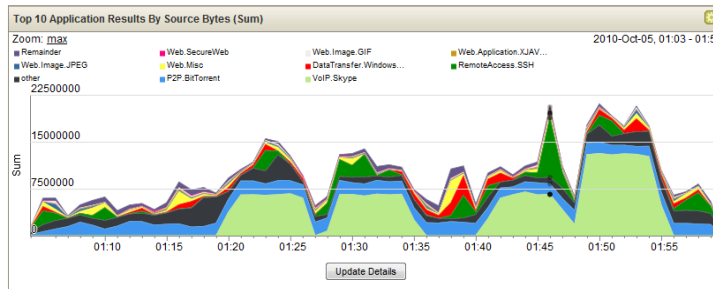
Application
Awareness

Vulnerability
Correlation

X-Force
Reputation

Example Network Anomaly uses cases

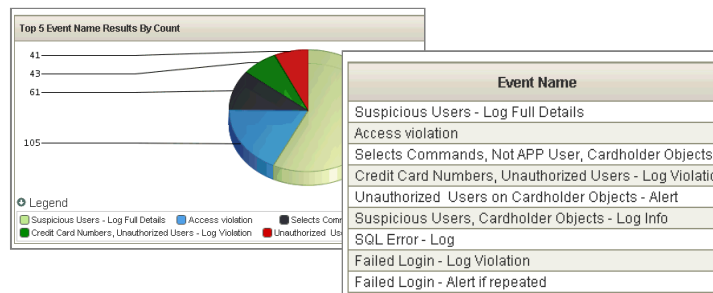
Behavior monitoring and flow analytics



Network Traffic Doesn't Lie

Attackers can stop logging and erase their tracks, but can't cut off the network (flow data)

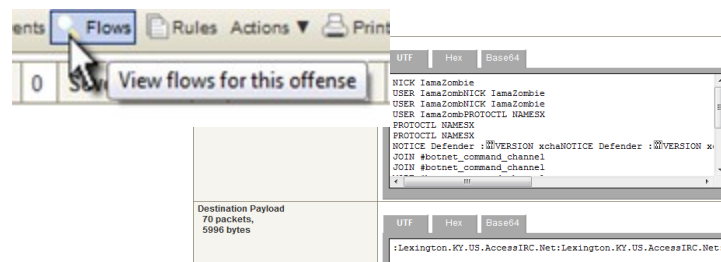
Activity and data access monitoring



Improved Breach Detection

360-degree visibility helps distinguish true breaches from benign activity, in real-time

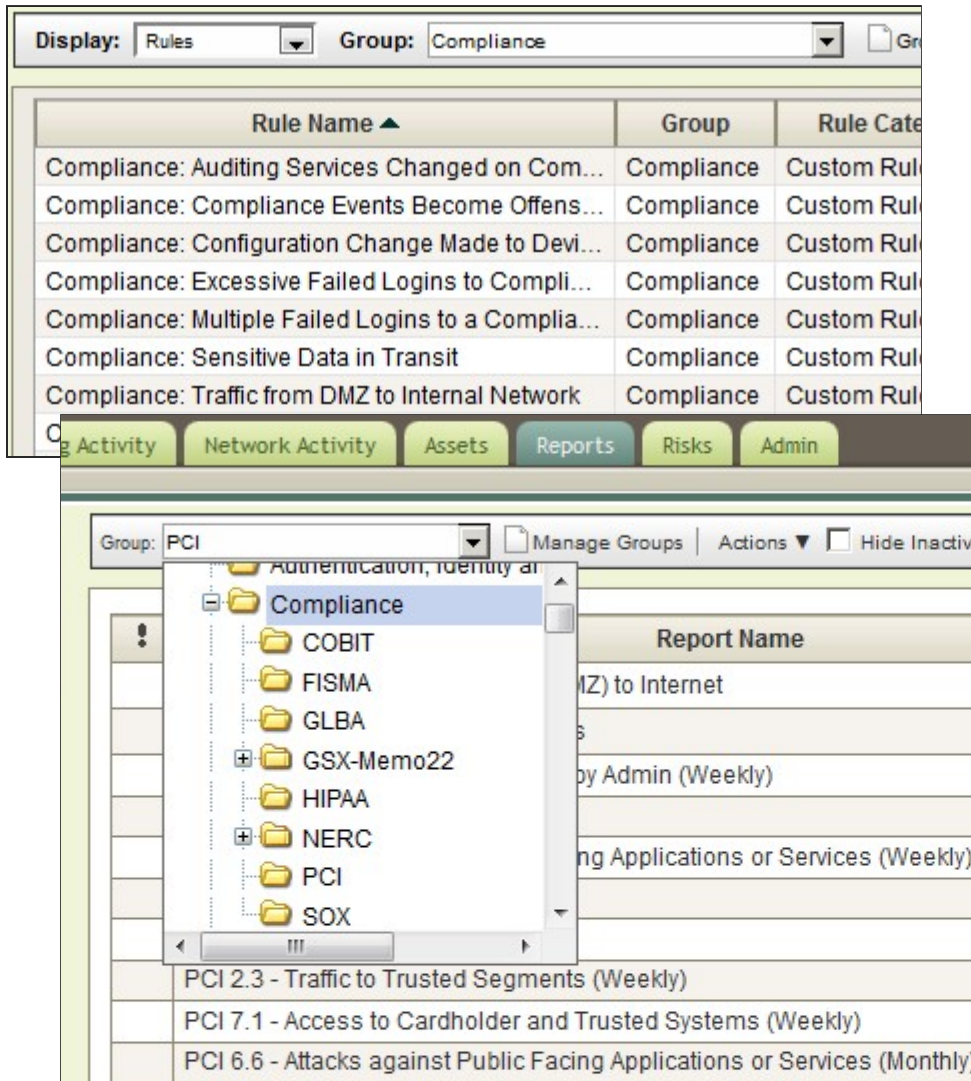
Stealthy malware detection



Irrefutable Botnet Communication

Layer 7 flow data shows botnet command and control instructions

Compliance Rules and Reports



The screenshot displays the IBM Security Systems interface. At the top, there are dropdown menus for 'Display: Rules' and 'Group: Compliance'. Below this is a table of compliance rules:

Rule Name ▲	Group	Rule Category
Compliance: Auditing Services Changed on Com...	Compliance	Custom Rule
Compliance: Compliance Events Become Offens...	Compliance	Custom Rule
Compliance: Configuration Change Made to Devi...	Compliance	Custom Rule
Compliance: Excessive Failed Logins to Compli...	Compliance	Custom Rule
Compliance: Multiple Failed Logins to a Complia...	Compliance	Custom Rule
Compliance: Sensitive Data in Transit	Compliance	Custom Rule
Compliance: Traffic from DMZ to Internal Network	Compliance	Custom Rule

Below the table is a navigation bar with buttons for 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Risks', and 'Admin'. The 'Reports' button is highlighted. Below the navigation bar, there is a 'Group: PCI' dropdown and a 'Manage Groups' button. A tree view shows a hierarchy of folders: 'Authentication, Identity and Access', 'Compliance', 'COBIT', 'FISMA', 'GLBA', 'GSX-Memo22', 'HIPAA', 'NERC', 'PCI', and 'SOX'. The 'Compliance' folder is expanded, showing a list of reports:

Report Name
DMZ) to Internet
S
by Admin (Weekly)
ng Applications or Services (Weekly)
PCI 2.3 - Traffic to Trusted Segments (Weekly)
PCI 7.1 - Access to Cardholder and Trusted Systems (Weekly)
PCI 6.6 - Attacks against Public Facing Applications or Services (Monthly)

- Templates for specific regulations and best practices:
 - COBIT, SOX, GLBA, NERC, FISMA, PCI, HIPAA, UK GCSx
- Easily modified to include new definitions
- Extensible to include new regulations and best practices
- Can leverage existing correlation rules



Dashboard

Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation

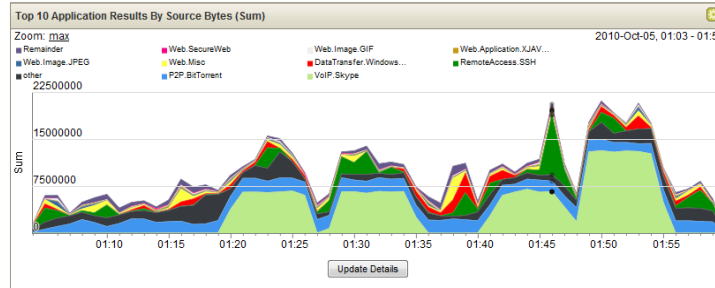
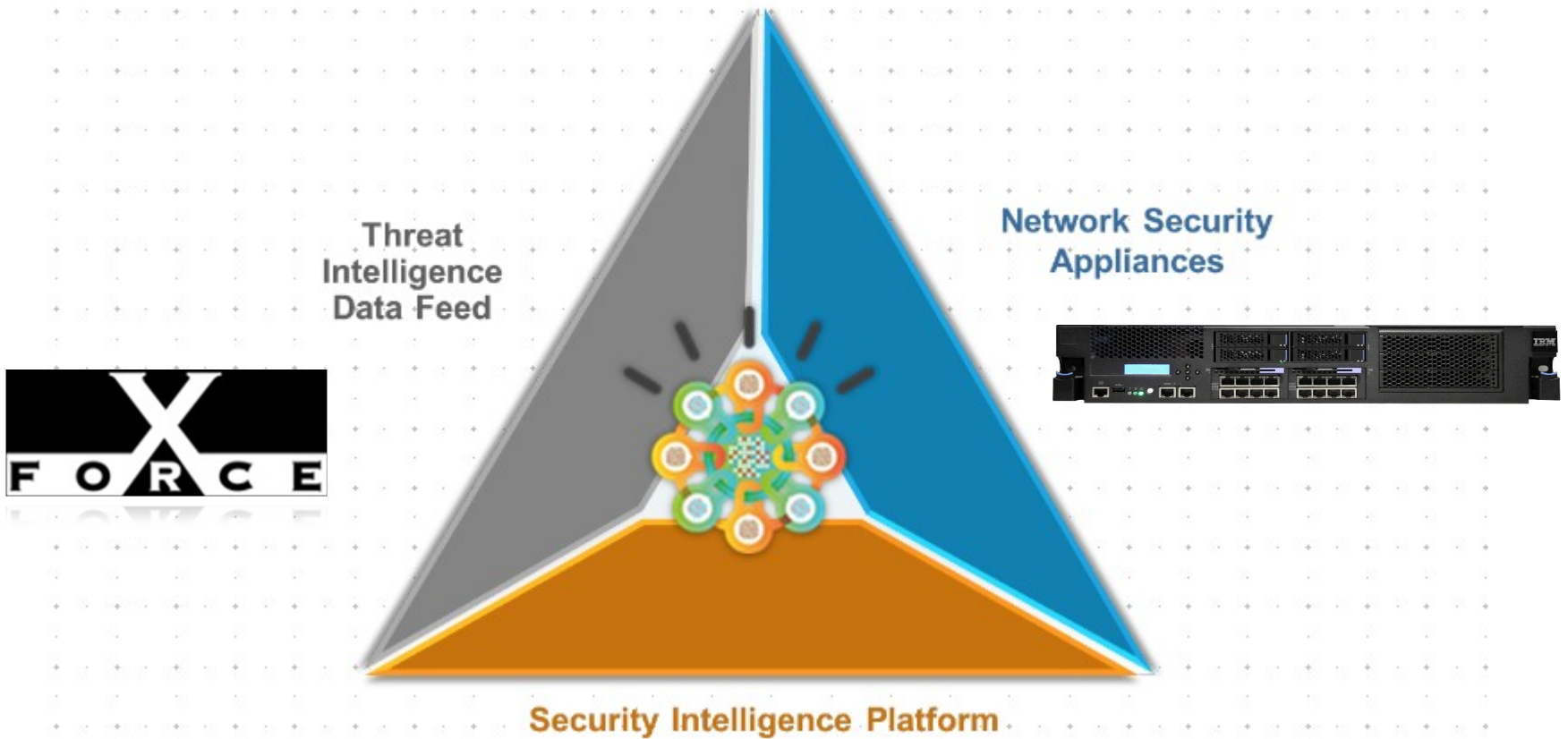


Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

Summary: Vision for Advanced Threat Protection





Thank you for visiting IBM® at AISA 2012.
We would appreciate your feedback below:

Mr / Mrs / Miss / Ms (Please circle one) _____

Name _____

Job Title _____

Company _____

Address _____

City _____ Postcode _____

Phone _____ Mobile _____

Email _____

*Terms and conditions apply. First 100 completed forms will receive complimentary gift.

IMPORTANT PRIVACY INFORMATION:
All fields are optional.
IBM and its affiliates may use the information you have provided to keep you informed about IBM products, services and offerings. By submitting this form I agree that IBM may process my data in the manner indicated above and as described in IBM's Privacy statement. You can request access to or correction of your details by calling IBM on 132 426 (Australia) or 0800 801 800 (New Zealand).

IBM values your feedback. Please take the time to complete this form.

Yes, I am interested in receiving communication relevant to my business via email from IBM

1. What is your purpose for attending AISA 2012?

- Thought leadership/education on directions of IT security
- Review or assess solutions for an existing business problem
- See what new security technologies are on offer
- Evaluate vendors for existing business problem & technical education
- Other _____

2. Please select your area/s of focus?

<input type="checkbox"/> Identity and access management	<input type="checkbox"/> Endpoint management
<input type="checkbox"/> Securing virtualised environments	<input type="checkbox"/> Data loss prevention
<input type="checkbox"/> Threat detection and prevention	<input type="checkbox"/> Single sign-on
<input type="checkbox"/> Log analysis and event aggregation	<input type="checkbox"/> Building Secure Applications
<input type="checkbox"/> Managed Security Services	<input type="checkbox"/> Cloud Security

3. Contact request

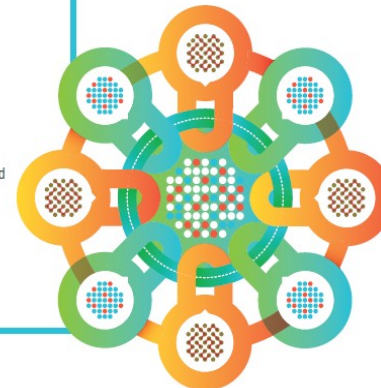
- I would like assistance in developing a business case
- I would like to book a demonstration of IBM solutions
- I would like a copy of IBM's latest expert analysis on security threats and vulnerabilities – the X-Force® IBM Trend and Risk report
- I would like to book a Security Assessment
- I would like a copy of the IBM presentation

4. Please add me to the IBM Security Newsletter distribution

Yes No

Comments

Thank you for your time.





ibm.com/security

© **Copyright IBM Corporation 2012. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.